REMARKS

By this Amendment, claims 31, 33-36, 38-61, 63-66, and 68-91 are now pending, with claims 31, 40, 61 and 70 amended, and with claims 32, 37, 62 and 67 cancelled. No new matter is introduced (see, e.g., claims 32, 37, 62 and 67, as previously presented). Reconsideration and allowance of the present case in view of the above amendments and following remarks is respectfully requested.

The rejection of (i) claims 31-32, 34-37, 41-45, 48-54, 56-58, 60-62, 64-67, 71-75, 78-84, 86-88, 90 and 91 based on *Comay et al.* (USP 6,363,489), (ii) claims 33, and 63 based on *Comay et al.* and *Cheng et al.* (USP 6,738,909), and (iii) claims 38-40, 46, 47, 55, and 59 based on *Comay et al.* and *Lyle* (USP 6,886,102) are respectfully overcome, because *Comay et al.*, *Cheng et al.*, and *Lyle*, taken alone or in combination, fail to disclose, teach or suggest all of the features recited in the claims. For example, independent claim 31, as amended (emphasis added) recites:

> A system for protecting a distributed network from unauthorized access, the system comprising:
>
> an intrusion detection system, including:
>
> an intrusion detection module, and
>
> a communications management module coupled to the intrusion detection module; and
>
> intrusion analysis system coupled to the intrusion detection system, and including:
>
> an intrusion analysis module, and
>
> an intrusion reaction coordination module coupled to the intrusion analysis module,
>
> wherein the intrusion detection module detects a possible unauthorized access attempt into or within a distributed network being protected,
>
> the communications management module is coupled to the intrusion analysis module and forwards to the intrusion analysis module information regarding the detected possible unauthorized access attempt,
>
> the intrusion analysis module determines based on the information regarding the detected possible unauthorized access attempt whether or not the detected possible unauthorized access attempt is authorized,
>
> if the intrusion analysis module determines that the detected possible unauthorized access attempt is authorized, the intrusion analysis module forwards, via the communications management module, information to the intrusion detection module that the possible unauthorized access attempt is authorized, and
>
> if the intrusion analysis module determines that the detected possible unauthorized access attempt is not authorized, **the intrusion analysis module determines, via the intrusion reaction coordination module, appropriate actions, including forwarding information regarding the detected unauthorized access attempt to a monitoring center external to the distributed network being protected**, and

processing information from the monitoring center regarding the detected unauthorized access attempt,

wherein **the intrusion analysis system in cooperation with the intrusion detection system enable communications between the monitoring center and an entity attempting the unauthorized access attempt without the entity being made aware that the entity attempting the unauthorized access attempt is communicating with the monitoring center**, and

the monitoring center sends information to the analysis system and intended for the entity attempting the unauthorized access attempt, the analysis system substitutes origin information of the monitoring center from the received information with origin information of a target of the unauthorized access attempt and forwards the substituted information to the entity attempting the unauthorized access attempt, whereby it appears to the entity attempting the unauthorized access attempt that communications are continuing with the target of the unauthorized access attempt; and

independent claim 61, as amended (emphasis added) recites:

A method for protecting a distributed network from unauthorized access for use in a system including an intrusion detection system having an intrusion detection module, and a communications management module coupled to the intrusion detection module, and intrusion analysis system coupled to the intrusion detection system, and including an intrusion analysis module, and an intrusion reaction coordination module coupled to the intrusion analysis module, the method comprising:

detecting, by the intrusion detection module, a possible unauthorized access attempt into or within a distributed network being protected;

forwarding, by the communications management module, information regarding the detected possible unauthorized access attempt to the intrusion analysis module;

determining, by the intrusion analysis module, based on the information regarding the detected possible unauthorized access attempt whether or not the detected possible unauthorized access attempt is authorized;

if the intrusion analysis module determines that the detected possible unauthorized access attempt is authorized, forwarding, by the intrusion analysis module, via the communications management module, information to the intrusion detection module that the possible unauthorized access attempt is authorized, and

if the intrusion analysis module determines that the detected possible unauthorized access attempt is not authorized, **determining, by the intrusion analysis module, via the intrusion reaction coordination module, appropriate actions, including forwarding information regarding the detected unauthorized access attempt to a monitoring center external to the distributed network being protected**, and processing information from the monitoring center regarding the detected unauthorized access attempt,

wherein **the intrusion analysis system in cooperation with the intrusion detection system enable communications between the monitoring center and an entity attempting the unauthorized access attempt without the entity being made aware that the entity attempting**

> **the unauthorized access attempt is communicating with the monitoring center**, and
>
> **the monitoring center sends information to the analysis system and intended for the entity attempting the unauthorized access attempt, the analysis system substitutes origin information of the monitoring center from the received information with origin information of a target of the unauthorized access attempt and forwards the substituted information to the entity attempting the unauthorized access attempt, whereby it appears to the entity attempting the unauthorized access attempt that communications are continuing with the target of the unauthorized access attempt**.

Thus, the invention recited in independent claims 1, and 61, as amended, includes the novel arrangement in the manner claimed and features thereof, for example, including forwarding information regarding a detected unauthorized access attempt to a monitoring center external to a distributed network being protected, and enabling communications between the monitoring center and an entity attempting the unauthorized access attempt without the entity being made aware that the entity attempting the unauthorized access attempt is communicating with the monitoring center, wherein the monitoring center sends information to the analysis system and intended for the entity attempting the unauthorized access attempt, the analysis system substitutes origin information of the monitoring center from the received information with origin information of a target of the unauthorized access attempt and forwards the substituted information to the entity attempting the unauthorized access attempt, whereby it appears to the entity attempting the unauthorized access attempt that communications are continuing with the target of the unauthorized access attempt.

By contrast, *Comay et al.* is directed to a method and a system for providing security to a network by identifying an unauthorized user who is attempting to gain access to a node on the network, and by then actively blocking that unauthorized user from further activities. Detection is facilitated by the unauthorized user providing a "mark", or specially crafted false data, which the unauthorized user gathers during the information collection stage performed before an attack. The mark is designed such that any attempt by the unauthorized user to use such false data results in the immediate identification of the unauthorized user as hostile, and indicates that an intrusion of the network is being attempted. The network is then blocked by diverting traffic from the unauthorized user to a secure zone, where the activities of the unauthorized user can be contained without damage to the network. However, *Comay et al.* fails to disclose, teach or suggest the novel arrangement and features thereof in the manner

recited in independent claims 1 and 61, as amended. Specifically, *Comay et al.* discloses at col. 5, lines 32-43 (emphasis added):

> Intrusion diversion module 26 optionally captures all packets, which feature the intruder-identifying factor, such as the source address of unauthorized source 20 for example. The received packets are then preferably handled proactively, and more preferably are redirected. Most preferably, such **redirection is performed such that the packet is redirected to a secure zone 32 within protected network 12**. First, the destination address of the received packet could optionally be changed to a secure address of a particular node 16 within secure zone 32. Next, the source address is changed to an intrusion diversion address assigned to intrusion diversion module 26.

Thus, *Comay et al.* not only fails to disclose, teach or suggest the novel arrangement and features thereof in the manner recited in independent claims 1 and 61, as amended, but also teaches away from same by disclosing the forwarding of information regarding a detected unauthorized access attempt is to a secure zone within rather that external to a protected network. Accordingly, in view of such teaching away, one of ordinary skill in the art would find no motivation to modify *Comay et al.* to include forwarding information regarding a detected unauthorized access attempt to a monitoring center external to a distributed network being protected, and the novel arrangement and features thereof in the manner recited in independent claims 1 and 61, as amended.

Lyle fails to cure the noted deficiencies in *Comay et al.* and is directed to a system and method for determining whether a sender seeking to send a message to a receiving computer system via a network is an authorized sender. A request to communicate is received from the sender. A number N1 is selected. A hash value for the number N1 is calculated. The hash value is sent to the sender. However, *Lyle* fails to disclose, teach or suggest the novel arrangement and features thereof in the manner recited in independent claims 1 and 61, as amended.

Cheng et al. fails to cure the noted deficiencies in *Comay et al.* and is directed to method and apparatus for use in data processing system for selecting rules to filter data for a tunnel, wherein a request is received to create a tunnel to another data processing system, a granularity of information about the data processing system is identified to form an identified granularity, the identified granularity of the information about the data processing system is used to select a rule, which matches the identified granularity, the rule is placed in a filter, and the filter associates data packets with the tunnel. However, *Cheng et al.* fails to disclose,

teach or suggest the novel arrangement and features thereof in the manner recited in independent claims 1 and 61, as amended.

Accordingly, independent claims 1 and 61, as amended, distinguish over the applied references, taken alone or in combination. The dependent claims are allowable over the applied references, taken alone or in combination, on their on merits, and for at least the reasons advanced with respect to independent claims 31 and 61.

In view of the foregoing, it is submitted that the present application is in condition for allowance and a notice to that effect is respectfully requested. However, if the Examiner deems that any issue remains after considering this response, the Examiner is invited to contact the undersigned attorney to expedite the prosecution and engage in a joint effort to work out a mutually satisfactory solution.

Respectfully submitted,

NIXON PEABODY, LLP

/Carlos R. Villamar, Reg. # 43,224/
Carlos R. Villamar
Reg. No. 43,224

NIXON PEABODY LLP
CUSTOMER NO.: 22204
401 9th Street, N.W., Suite 900
Washington, DC 20004
Tel: 202-585-8000
Fax: 202-585-8080